On the Vulnerability of Smart Card Transactions

Author: Lai Man Tang

Department of Computer and Information Science

Indiana University-Purdue University Indianapolis

Abstract:

The number of non-cash transactions is increasing every year at a rapid pace because of the underlying flexibility in the payment mechanism and the improved reliability and protection offered by many networks and debit and credit card issuers and acquirers. According to a study by Capgemini, the growth of the number of non-cash-based transactions per inhabitant in the United States increased by 40% from 2012 to 2013. This clearly indicates a strong shift towards a cashless society.

However, the above trend is also coupled with an increasing trend in card fraud schemes ranging from gas pump skimmers to application fraud. Even the most recent chip and pin technology has been the victim of fraud as detailed in performing a man-in-the-middle attack by inserting a programmed chip called FUN card.

In this study, we investigate the functionalities of smart cards and their susceptibility to fraud based on interference at the hardware level. We specifically analyze processor cards with a cryptographic processors and research the possibility to change the behavior of the hardware either in offline or online transactions in way that may be able to reveal the private key used to authenticate the transaction between the acquirer and the issuer. The results of these investigations can be used to enhance the current encryption as well as the authentication mechanisms used in card transactions.